U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Law Enforcement Training System (LETS)
Bureau/Office: U.S. Fish and Wildlife Service (FWS)
Date: [of last signature]
Point of Contact:
Name: Jennifer Schmidt
Title: FWS Privacy Officer
Email: fws_privacy@fws.gov
Address: 5275 Leesburg Pike, MS: IRTM, Falls Church, VA 22041

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Law Enforcement Training System (LETS) is used by the Fish and Wildlife Service (FWS) Office of Law Enforcement (OLE) Training & Inspection division to help manage its training operations for FWS Law Enforcement Officers (LEO), other Federal LEOs and local, state, Tribal, and international LEOs responsible for the enforcement of wildlife laws in the U.S. and abroad.

C. What is the legal authority?

5 U.S.C. 4101, et seq., Government Organization and Employee Training; 5 U.S.C. 1302, 2951, 4118, 4506, 3101; 43 U.S.C. 1457; Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. 2000d); Executive Order 11348, Providing for Further Training of Government Employees, as amended by Executive Order 12107, Relating to Civil Service Commission and Labor Management in Federal Service; 5 CFR 410, Subpart C, Establishing and Implementing Training Programs and the E-Government Act of 2002 (44 U.S.C. 3501, et seq.).

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No – LETS is in the process of CSAM registration.

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None.			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

INTERIOR/FWS-20, Investigative Case Files (June 4, 2008) 73 FR 31877. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in

accordance with OMB Circular A-108. This system is exempt from portions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

LETS is in the process of receiving OMB approval.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name	☐ Religious Preference	☐ Social Security Number (SSN)
☒ Citizenship	☐ Security Clearance	☐ Personal Cell Telephone Number
☒ Gender	☐ Spouse Information	☐ Tribal or Other ID Number
☒ Birth Date	☐ Financial Information	☐ Personal Email Address
☐ Group Affiliation	☐ Medical Information	☐ Mother's Maiden Name
☐ Marital Status	☐ Disability Information	☐ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☐ Other Names Used	☐ Law Enforcement	☒ Employment Information
☐ Truncated SSN	☐ Education Information	☐ Military Status/Service
☐ Legal Status	☒ Emergency Contact	☐ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	☐ Race/Ethnicity

☒ Other: *Specify the PII collected.*

Official phone numbers, mailing and email addresses, and LETS username and password.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency – DOS vetted
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☒ State agency

☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☐ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Once students are approved by their supervisor (domestic) or vetted by the Department of State (international), OLE staff manually loads their names and email addresses into LETS. Students are then emailed a secure link where they complete registration and set up secure access to the system.

D. What is the intended use of the PII collected?

The PII in LETS is used to manage administrative functions of OLE's Training and Inspection Division including but not limited to: student registration, scheduling and coordination of internal and external training events; testing and surveying students, as well as maintaining required law enforcement training records throughout the career of OLE personnel.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☐ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☐ Contractor: *Describe the contractor and how the data will be used.*

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

A Privacy Act statement and notice of monitoring is available for students to read at the LETS registration and login pages. DOI/FWS employees (including law enforcement) receive notice and consent to the specific uses of their PII during the hiring and onboarding process. Students external to DOI may decline to provide their information; however, they will not be granted access to the system or able to register and attend training.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records may be searched for and retrieved by the student's full name, course name, location, etc.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Upon authorized request, LETS can generate an individual's training record. These records include the names and dates of all (FWS) courses attended, pre- and post-test scores, and any incomplete training upon authorized request.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The individuals will be provided a secure link to their official email address and be required to complete/input their own data into the database and affirm that it is accurate.

B. How will data be checked for completeness?

LETS utilizes required fields so that all necessary information must be filled out by the students before they can move forward to the next question. They will not be able to submit the document until all required fields are completed and validated by the student for completeness and accuracy.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Records will be disposition when they have reached the end of their business need, have met the approved records schedule time frame, and are not under any litigation holds. Request for destruction will be approved by the Bureau Records Officer, or their designated Official. Authorization for disposition is found in 283 FW1, Disposition Program, 44 U.S.C. 3302 Disposal of Records, and 36 CFR 1228 Disposal of Federal Records.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1. Dispositioning of records will be accomplished within the automated records retention functions built in the system and procedures will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, Departmental guidance, and the FWS Records Schedule.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Mitigation – DOS vetting, only collected from individual
Very limited admin rights
Disclosures approved by SAC and in coordination FOIA

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

FWS has oversight responsibilities under statutory and regulatory authority to regulate the importation, exportation, and transportation of wildlife. FWS' inspection program is framed by the Endangered Species Act and the Lacey Act amendments of 1981. FWS is also charged with enforcing Federal wildlife laws and protecting natural resources, visitors and employees on National Wildlife Refuge System lands.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No – not applicable, LETS does not derive new data or create previously unavailable data about an individual.

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No – not applicable, LETS does not derive new data or create previously unavailable data about an individual.

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access control, least privilege, etc.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The system maintains an audit trail of users' critical activities.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The audit trail logs administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, permission changes and access history.

M. What controls will be used to prevent unauthorized monitoring?

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☐ Identification Badges
☐ Safes
☐ Combination Locks
☐ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☐ Password
☐ Firewall
☐ Encryption
☐ User Identification
☐ Biometrics
☐ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☐ Personal Identity Verification (PIV) Card

☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☐ Periodic Security Audits
☐ Backups Secured Off-site
☐ Rules of Behavior
☐ Role-Based Training
☐ Regular Monitoring of Users' Security Practices
☐ Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Encryption of Backups Containing Sensitive Data
☐ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Section 5. Review and Approval

Information System Owner

Name: _____
Title: _____
Bureau/Office: _____
Phone: _____ Email: _____

Signature: _____ Date: _____

Information System Security Officer

Name: _____
Title: _____
Bureau/Office: _____
Phone: _____ Email: _____

Signature: _____ Date: _____

Privacy Officer

Name: _____
Title: _____
Bureau/Office: _____
Phone: _____ Email: _____

Signature: _____ Date: _____

Reviewing Official

Name: _____
Title: _____
Bureau/Office: _____
Phone: _____ Email: _____

Signature: _____ Date: _____